PENTESTERRA

WEB & API PENTEST

La Tua App Resiste a un Attacco Vero?

Penetration test su applicazioni web e API - testato come farebbe un attaccante, con exploit reali, non solo una scansione automatica con un report generico.

COS'È UN WEB/API PENTEST, IN BREVE

È una verifica attiva della sicurezza informatica (cyber) della tua applicazione web e delle sue API - SQL injection, autenticazione rotta, controllo accessi, logica di business - fatta tentando di sfruttare davvero le falle, non limitandosi a segnalarle. È l'evidenza tecnica che NIS2, PCI DSS e quasi ogni framework di cybersicurezza richiedono.

60+
Moduli di attacco su 21 classi di vulnerabilità testate attivamente

REST + GraphQL
API moderne testate quanto l'applicazione web

Verificato
Ogni finding critico ha una prova di sfruttabilità reale

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO, il responsabile IT o il CTO di un'azienda che espone un'applicazione web o delle API ai propri clienti, partner o dipendenti - e che deve sapere se un attaccante potrebbe davvero entrarci.

COSA È SUCCESSO

Una nuova funzionalità è stata rilasciata l'ultimo sprint, e nessuno l'ha ritestata da un punto di vista di sicurezza. Le API sono cresciute di trimestre in trimestre, e metà di esse non è nemmeno documentata in una specifica che qualcuno mantiene davvero.

IL PROBLEMA

Non sai, con certezza, se la tua applicazione e le tue API resistono a un attacco reale di cybersicurezza. Un endpoint non documentato con un controllo di autorizzazione rotto è invisibile a uno scanner basato su specifica - ed è esattamente ciò che un attaccante trova per primo.

PERCHÉ FA MALE

La maggior parte delle violazioni applicative non arriva dalla classe di vulnerabilità testata l'anno scorso - arriva dall'endpoint che non esisteva ancora quando è stato fatto l'ultimo test. Un cliente enterprise, un assicuratore cyber o un auditor possono chiedere prova di un penetration test recente prima di firmare.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con prova concreta, quali falle nella tua applicazione e nelle tue API sono realmente sfruttabili - non una lista di avvisi teorici basati su una specifica statica.

LA SOLUZIONE

Un **Penetration Test** completo su applicazione web e API - REST, GraphQL, WebSocket - con exploitation reale e non distruttiva su injection, autenticazione, controllo accessi e logica di business, e scoperta automatica della superficie API da specifiche, bundle JavaScript e traffico osservato.

PERCHÉ È DIVERSO

Non stai comprando l'ennesima scansione automatica con falsi positivi. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. Molti dei tuoi concorrenti diretti si stanno già rivolgendo a noi. E il test include l'analisi autenticata dei tuoi flussi utente reali - pagamenti, operazioni admin, gestione dati - così un IDOR su un endpoint di pagamento viene segnalato come rischio di frode finanziaria, non come "severità media" generica: è la classe di finding che un pentester manuale esperto individua e uno scanner automatico si lascia sfuggire.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con ogni finding critico verificato tramite un proof-of-concept reale. Se emergono gap più ampi, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment di rete, penetration test infrastrutturale, formazione anti-phishing.

~15 min

Tempo medio per i primi findings, dall'avvio del test

JWT · OAuth

Autenticazione e trust boundary testati a fondo

Non distruttivo

Nessun rischio per l'ambiente di produzione

COSA INCLUDE DAVVERO

Test attivo con exploit reali su 21 classi di vulnerabilità - non un pattern-matching passivo contro una checklist statica.

Injection e lato client

I percorsi di exploit ad alto impatto e la superficie di attacco lato client, testati attivamente.

- SQLi (error/boolean/time-based), NoSQLi ed escalation a RCE, SSTI, XXE, prototype pollution
- XSS reflected, stored e DOM con bypass CSP, DOM clobbering, injection via postMessage
- Command injection, upload file non ristretto, injection di secondo ordine

Infrastruttura web e cloud

Il livello edge, cache e cloud-native che molti scanner ignorano completamente.

- HTTP request smuggling, cache poisoning, web cache deception
- SSRF/RFI con pivoting su IMDS v1/v2 AWS/GCP/Azure, esposizione dei metadati cloud
- Misconfigurazione CORS, host-header injection, subdomain takeover

AI, logica di business e minacce emergenti

I rischi a livello applicativo emersi dagli incidenti reali degli ultimi due anni.

- Prompt injection su LLM/AI (OWASP LLM01:2025)
- IDOR, broken authorization, mass assignment, workflow aggirabili, difetti di state transition
- Attacchi di downgrade WebAuthn/passkey, ReDoS

Verifica prima di tutto, consapevole del WAF

Un finding non è una vulnerabilità finché non è confermato da un exploit reale.

- Fingerprinting dello stack tecnologico, rilevamento WAF/CDN con evasione adattiva del payload
- Ogni finding passa dalla pipeline di verifica - PoC allegato, non solo un'etichetta di severità
- Esecuzione distribuita su più nodi scanner, nessun collo di bottiglia

PENTESTERRA

WEB & API PENTEST

COSA RICEVI

- ✓ Un report PDF completo con ogni vulnerabilità confermata e la relativa prova
- ✓ Copertura di SQL injection, XSS, autenticazione, autorizzazione, logica di business
- ✓ Analisi specifica delle API REST, GraphQL e WebSocket
- ✓ Raccomandazioni di remediation prioritizzate per rischio reale
- ✓ Executive summary pronto per il tuo consiglio o per un cliente enterprise

COME FUNZIONA

1

Definiamo il perimetro

Applicazione web, API, o entrambe - stabiliamo insieme lo scope del test.

2

Scopriamo la superficie

Mappiamo endpoint documentati e non, comprese le API dimenticate.

3

Testiamo attivamente

Tentiamo lo sfruttamento reale, in modo sicuro e non distruttivo.

4

Ti consegniamo il report

Un PDF completo con i rischi prioritizzati e le azioni da intraprendere.

Scopri se la tua applicazione resiste a un attacco vero

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi il tuo Web/API Pentest →

info@pentesterra.com · pentesterra.com/web-app-pentest